Doc. Ing. Roman Rak, Ph.D.
Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c.

VERIFIKACE OSOBY NA ZÁKLADĚ OVĚŘOVÁNÍ JEJÍHO PODPISU

1. ÚVOD

V souvislosti s ručně psaným písmem rozeznáváme několik základních úloh, které jsou předmětem intenzivního vědeckého výzkumu a následně tvorby sofistikovaných aplikací z oblasti umělé inteligence, jež nacházejí stále širší uplatnění v každodenní praxi. Středem pozornosti jsou převod ručně psaného písma do klasického formátu běžných textových editorů, rozpoznávání obsahu ručně psaného písma a další následné operace (např. strojové překlady) – tyto dvě úlohy jsou úzce spojeny. Dále sem zařazujeme ověření identity osoby s možnou dalších specifikací jejich osobnostních rysů vycházejících z grafické formy jejího písma a v neposlední řadě identifikace/verifikace osoby na základě jejího podpisu.

Obr. 1 Ukázky různých technologií digitálního snímání podpisu osoby.

Následující text bude zaměřen právě na nejrůznější identifikačně-verifikační metody spojené s behaviorálními biometrickými charakteristikami podpisu.

Automatizovaná verifikace založená na rozpoznávání podpisu prověřované osoby patří k nejpraktičtějším způsobům ověřování lidské identity. Podpis nemůže být ztracen, odcizen nebo zapomenut a jeho základní výhoda spočívá v jeho přirozenosti při používání v běžném životě, při každodenních operacích. Ověřování podpisu může být proto využito v klasických oblastech, jako jsou bezpečnost, kontrola přístupu nebo finanční či kontraktační transakce.

Biomechanický proces vzniku lidského podpisu není nikterak jednoduchý. Jeho základní popis je uveden v [1] následujícím způsobem: Primární vzruch vzniká v centrálním nervovém systému – v lidském mozku s předem definovanou intenzitou a trváním. Nervový systém pak aktivuje příslušné svaly v definovaném pořadí. Pohyb pera po papíře, což je výsledek stahování a uvolňování svalů, zanechává stopu hrotu psacího nástroje.

Návrh a výsledné řešení automatizovaných systémů na rozpoznávání osoby podle podpisu (či písma) vychází z toho, že lidský rukopis není nijak standardizovaný či stejný, ale naopak je velmi individuální.

V principu existují dva základní typy systémů na rozpoznávání osoby podle podpisu: on line systémy a off line systémy.

1.1 Off line systémy pro verifikaci osob podle jejího podpisu

U off line systémů verifikovaná osoba se podepisuje klasickým způsobem na papír. Následně je podpis digitalizován prostřednictvím optického skeneru nebo kamery. Dále pak aplikace určuje shodnost podpisu osoby s referenčním vzorkem na základě srovnání celkového tvaru (obrazu) podpisu.

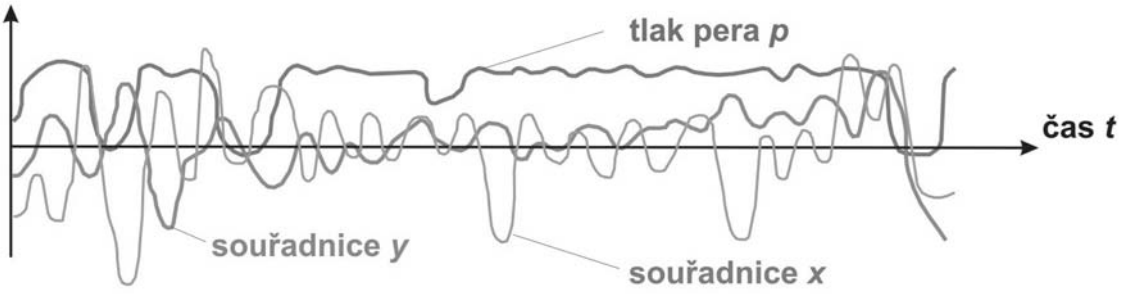
1.2 On line systémy pro verifikaci osob podle jejího podpisu

U on line systémů jsou charakteristiky právě psaného podpisu získávány v reálném čase pomocí specializovaného tabletu, nebo speciálně upraveného pera či jiným specifickým snímacím hardwarem. Všechna tato zařízení zachycují statické i dynamické charakteristiky podpisu v průběhu jeho samotného vzniku.

1.3 Statické a dynamické systémy pro verifikaci osoby podle podpisu

On line systémy pro proces vyhodnocování osoby pak využívají jak statické, tak i dynamické informace. *On line systémy se* proto také někdy nazývají *dynamické systémy* pro ověřování osoby podle

Doc. Ing. Roman Rak, Ph.D., manažer kompetenčního centra vnitropodnikových aplikací, Telefonica O_2 Czech Republic, Olšanská 5, 130 00 Praha 3, e-mail: roman.rak@o2.com
Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c., Katedra trestního práva, kriminalistiky a forenzních disciplín, Vysoká škola Karlovy Vary, o. p. s., T. G. Masaryka 3, 360 01 Karlovy Vary, e-mail: viktorporada@vskv.cz



Obr. 2 Dynamické vlastnosti podpisu.

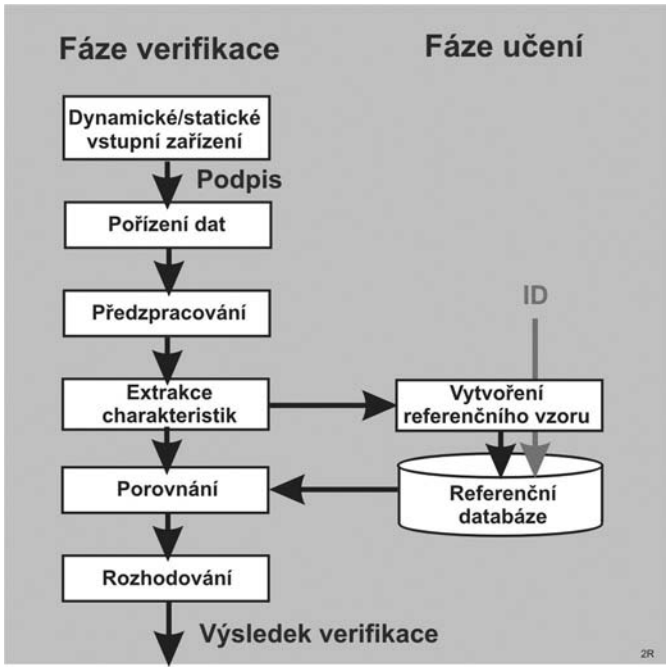
podpisu, zatímco *u off line systémů* se můžeme setkat s pojmem *statický systém*.

2. ZÁKLADNÍ ETAPY VERIFIKACE OSOBY

Proces verifikace osoby podle jejího podpisu se často skládá ze dvou základních etap: z etapy učení a z etapy testování (vlastní verifikace podpisu), tak jak je znázorněno na obr. 3.

V etapě učení verifikační systém používá extrahované charakteristiky z jednoho nebo více pokusných vzorků, aby si vytvořil referenční databázi podpisu. Každé podpisující se osobě je přiděleno vlastní identifikační číslo (ID). Toto ID je použito jako unikátní identifikační klíč pro podpisující se osobu a je spojeno (databázově linkováno) se vzorem jejího referenčního podpisu.

V etapě testování (verifikace podpisu) podpisující osoba předkládá své ID a podpisuje se na vstupním zařízení. Vzápětí verifikační systém na základě předloženého ID vyhledává v referenční databázi vzorový podpis a ten porovnává s charakteristikami podpisu sejmutého ze vstupního zařízení. Výsledkem tohoto porovnání je výrok, zda osoba byla verifikována (ověřena) či nikoliv. V prvním případě je daná osoba ověřena pro definované aktivity, zatímco ve druhém případě je jí k těmto aktivitám odmítnut přístup – osoba není právoplatným uživatelem daných činností.



Obr. 3 Základní etapy verifikace na základě podpisu.

Každý verifikační systém musí mít schopnost zabránit padělkům podpisů. V odborné literatuře jsou uváděny tři základní typy falzifikátů podpisu:

1. *„Jednoduchý“* padělek (ztožnění s jiným podpisem). „Padělatel“ (v tomto případě se nejedná o padělatele v pravém smyslu slova) nečiní žádné vědomé pokusy napodobit podpis oprávněné osoby. Podpis se zcela náhodně shoduje s podpisem jiné osoby, který je již uložen v databázi.
2. *„Substituční“* nebo *„nahodilý“* padělek. Osoba systému vědomě předkládá svůj podpis a záměrně tak zkouší, zda v referenční databázi není někdo jiný, kdo má stejný podpis. V případě že ano, vstoupila by do systému pak s identitou někoho zcela jiného, než je ona sama. Padělatel dopředu neví, za koho se bude vydávat. Krádež identity je necílená na konkrétní osobu.
3. *„Záměrně vytvořený“* padělek. Padělatel se zcela cíleně snaží napodobit statistické a dynamické charakteristiky podpisu osoby, za kterou se chce vydávat. Krádež identity je cílená na zcela konkrétní osobu.

Abychom zabránili průniku neoprávněné osoby do chráněné aplikace, prostoru či k určité aktivitě, verifikační systém musí být správně nastaven, tj. musí být vhodně zvoleny hodnoty statistických veličin FAR a FRR[1)].

2.1 Off line systémy pro verifikaci osob podle jejího podpisu

U off line systémů je podpis napsán na papír a digitální data o jeho obrazu jsou získána skenováním nebo snímáním kamerou. Vstupní data jsou pak obrázkem podpisu $L(x, y)$ s příslušnými souřadnicemi x, y pro každý bod podpisu.

Off line systémy na verifikaci osoby podle jejího podpisu nejsou dnes pro automatizované zpracování zcela vhodné. Důvodem je nevhodnost samotného principu porovnání dvou statických obrazů podpisu (předkládaného vzoru s referenční šablonou), který je v době běžně dostupných skenovacích zařízení náchylný k podvrhům falzifikátů. Není totiž nijak nesnadné získat skenováním nebo fotografováním podpis osoby, za kterou se chceme vydávat a tento vzorek pak předložit snímacímu zařízení verifikační aplikace.

[1)] FAR – False Acceptance Rate; FRR – False Reject rate.

Obr. 4 Statické charakteristiky podpisu.

Obr. 5 Statické charakteristiky podpisu.

U moderních verifikačních systémů je požadován test „živosti" předkládaného vzorku, který je splněn právě v dynamických (on line) verifikačních systémech, kde je vyhodnocováno vedení tahu podpisu v souřadnicích *x, y* ve vztahu k času *t*, tlaku *p* hrotu psacího nástroje po celé trajektorii podpisu apod.

Off line systémy mají dnes své opodstatnění především ve forenzní praxi, kde se určuje identičnost podpisu ve vztahu k určité osobě pro potřeby samotného vyšetřování nebo jako soudní důkaz.

Automatizované prostředky pro verifikaci osoby podle podpisu se zpravidla skládají ze tří základních etap, kterými jsou:

- Předzpracování.
- Extrakce biometrických charakteristik.
- Vyhodnocování.

2.1.1 Předzpracování

V této etapě se používají standardní algoritmy jako jsou vyhlazování, zjednodušování a skeletizace, segmentace, normalizace apod. V reálných systémech ne vždy všechny tyto algoritmy jsou nezbytně nutné. Záleží především na tom, jaké charakteristiky podpisu chceme získat a jak dále s nimi budeme pracovat.

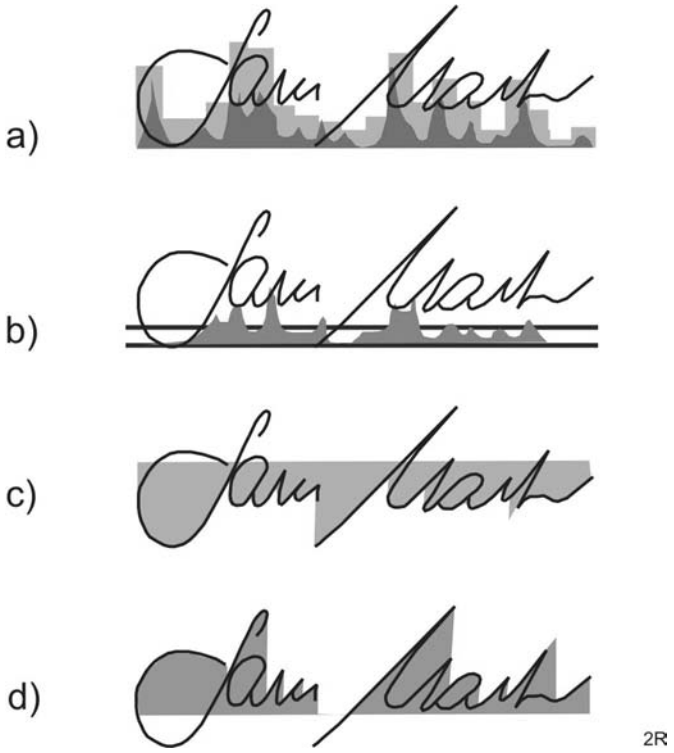
- *Prahování.* Každý pixel obrazu v celém svém spektru šedivosti je porovnáván s definovaným prahem. V závislosti, zda prahovou hodnotu převyšuje či nikoliv, je zařazen do jedné ze dvou kategorií (0, 1). Po prahování obraz podpisu v různých odstínech šedi je přeměněn do svého binárního obrazu.
- *Vyhlazování a normalizace.* Technika vyhlazování se používá ke zbavení se nevýznamných oblastí šumu v obraze. Následně se pak zpravidla používá i normalizace. Po normalizaci je obraz převeden do určitého relativního měřítka. Normalizační metody bývají dvojího druhu – lineární a nelineární.
- *Zjednodušování.* Tato technika se používá ke zjednodušení obrazové scény podpisu. Po zjednodušení šířka tahu hrotu psacího nástroje podél celé trajektorie podpisu je změněna na jediný pixel, takže vznikne jen základní kostra (skelet) podpisu.

2.1.2 Extrakce biometrických charakteristik

Charakteristiky podpisu u off line verifikačních systémů mohou být klasifikovány dvěma základními typy: *textově nezávislé* a *textově závislé charakteristiky*.

Textově nezávislé charakteristiky jsou ty charakteristiky, jež nijak nezávisí na tom, co lidé píší, jaký je obsah písemného sdělení. Extrakce textově nezávislých charakteristik obvykle využívá texturové analýzy, transformačních metod a histogramů. V práci [3] se využívá nízkofrekvenčního pásma Fourierova spektra a příslušné charakteristiky jsou extrahovány z frekvenční distribuce globálních nebo lokálních vlastností. Tyto metody jsou ale pro detailní analýzu podpisu poměrně hrubé či jen přibližné a rozlišovací schopnost rozpoznat dva odlišné podpisy je velmi slabá.

Textově závislé charakteristiky zcela závisí na tom, co lidé píší. Většina textově závislých charakteristik má geometrické a topologické rysy. Různé metody a přístupy statické analýzy písma využívají nejrůznější uzavřené smyčky a speciální body, jako jsou hraniční nebo křižující se body na křivce podpisu [4, 5]. Jiné metody a přístupy využívají různé plochy, které vznikají jako oblasti ohraničené uzavřenou křivkou podpisu, např. horní a spodní uzavřené plochy (obr. 6) [6]. Tvar podpisu může být popisován pomocí souřadnicových mřížek nebo textur [4]. Některé metody na základě statického obrazu podpisu dokonce dokáží odvozovat dynamické vlastnosti podpisu jako je tlak na hrot psacího nástroje nebo časové údaje (rychlost psaní křivky v různých místech) [6, 7].



Obr. 6 Grafické znázornění některých statických charakteristik písma: a) hustota a vektor linie tahu, b) vertikální hustota linie tahu, c) horní uzavřená oblast vektorů, d) dolní uzavřená oblast vektorů.

Společné využívaní textově závislých a textově nezávislých charakteristik zajišťuje vyšší rozlišovací schopnost off line verifikace osoby založené na lidském podpisu.

2.1.3 Vyhodnocování

Off line metody vyhodnocování podpisu jsou založeny na vyhodnocování vektorů charakteristik. Nejrozšířenějšími algoritmy jsou převážně založeny na statistických přístupech a na umělé neuronové síti[2].

Statistické metody pro off line verifikaci podpisu jsou založeny na klasifikátoru nejbližšího souseda (*nearest neighbor classifier*), K-klasifikátoru nejbližšího souseda (*K-nearest neighbor classifier*), na lineárním a prahovém klasifikátoru. Neuronové sítě využívají fuzzy ARTMAP metodiku, zpětnovazební neuronovou síť či mnohovrstvou neuronovou síť.

Obr. 7 Grafická ukázka filosofie porovnání dvou podpisů.

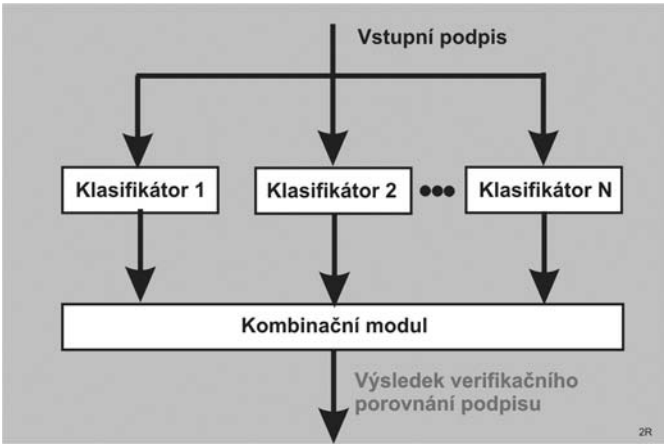
Některé metody jsou v odborné literatuře stručně popisovány takto:

a) *Porovnání významových bodů.* V této metodě je linie tahu podpisu ztenčena a jsou z ní extrahovány speciální body, jako jsou např. koncové body, body ve kterých se tah psacího nástroje obrací, body ve kterých se tah kříží apod. Finální porovnávání pak určuje míru ztotožnění významových bodů předloženého podpisu s podpisem referenčním.

b) *Klasifikátor souseda.* Off line pořízené podpisy jsou reprezentovány vektorem jejich vlastností. V praxi se běžně používají dva klasické statistické algoritmy: klasifikátor nejbližšího souseda a K-klasifikátor nejbližšího souseda. Předložený podpis verifikované osoby je porovnán se všemi referenčními podpisy a je vyhodnocen nejbližší (nejpodobnější) podpis (nebo podpisový – referenční vzor s největším počtem K nejbližších referenčních podpisů).

c) Neuronové sítě. Nejběžnější metodou v praxi jsou neuronové sítě. V některých metodikách jsou jako datový vstup do neuronové sítě používány vektory vlastností podpisu získané již ve fázi extrakce charakteristik, v jiných metodických postupech jsou nezbytné charakteristiky extrahovány až v procesu vyhodnocování pomocí neuronových sítí.

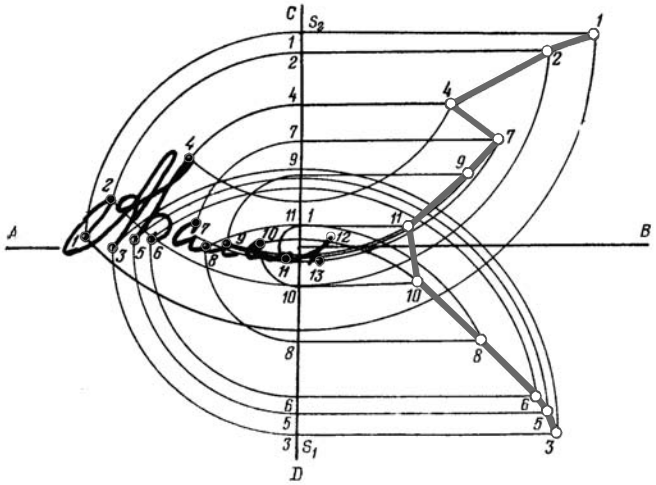
[2] Artificial Neural Network – ANN.



Obr. 8 Základní schéma kombinace dílčích klasifikátorů.

Aby se efektivita vyhodnocování podpisu zvýšila, v praxi se běžně kombinují metody s několika typy klasifikátorů [4, 6, 9, 10]. Obr. 8 znázorňuje jejich základní architekturu. Každý klasifikátor v tomto schématu vyhodnocuje podpis zcela nezávisle. Výsledek je pak založen na vahách, přidělených jednotlivým klasifikátorům.

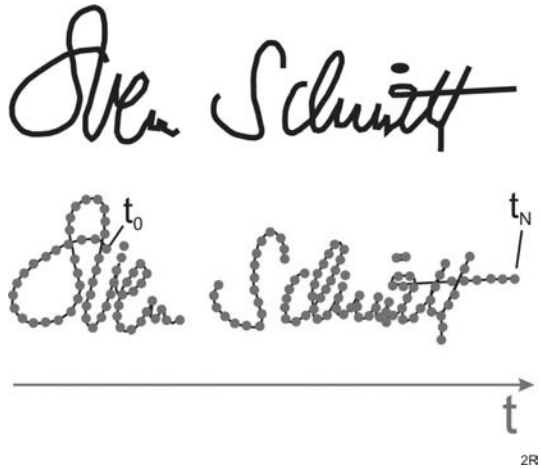
V sedmdesátých letech minulého století sovětská kriminalistická škola používala grafickou identifikační analýzu (známou pod zkratkou GIA). Podstata této metody byla založena na porovnání dvou normalizovaných determinantů. Metoda sama při finálním zpracování nepoužívala žádný matematický aparát, ale pouze se vynášely klíčové charakteristiky podpisu podle předem definované logiky. Základní ukázka je znázorněna na obrázku obr. 9.



Obr. 9 Ukázka grafické identifikační analýzy (GIA) s výsledným srovnávacím determinantem (svislá lomená linie vpravo). Ten je následně graficky ztotožňován s determinantem jiného podpisu.

2.2 On line systémy pro verifikaci osob podle jejího podpisu

On line verifikační systémy založené na podpisu se od off line systémů liší způsobem získávání dat. U on line systémů jsou data získávána v reálném čase pomocí digitalizačního tabletu



Obr. 10 Podpis je u on-line systémů vnímán jako množina funkcí závislých na čase. V každém okamžiku t jsou snímány dynamické hodnoty v konkrétních bodech: t_0 – začátek podpisu, t_N – ukončení podpisu.

nebo pomocí speciálního pera. Dynamické, on line systémy tedy nezískávají jenom obrazovou podobu podpisu, ale také dynamické charakteristiky. Bylo již zmíněno, že právě tyto dynamické charakteristiky odrážejí unikátní zvyky podpisující se osoby a je tedy mnohem složitější falšovat podpis [11]. K dynamickým vlastnostem patří rychlost psaní, tlak pera v jednotlivých bodech trajektorie, pořadí psaní jednotlivých částí podpisu apod.

On line systémy jsou obvykle chápány nebo representovány pomocí matematické časové funkce $F(t)$. Obr. 10 představuje ukázku on line podpisu, kde jednotlivé tečky ukazují umístění hrotu pera v daném čase. Úsečky spojují jednotlivé body v časové posloupnosti.

Jedním z důležitých cílů využití dynamických charakteristik podpisu je detekovat případné podvrhy či napodobeniny podpisu. V následujících odstavcích jsou stručně popsány základní etapy činnosti on line systémů pro verifikaci osoby podle jejího podpisu.

2.2.1 Předzpracování a extrakce charakteristik

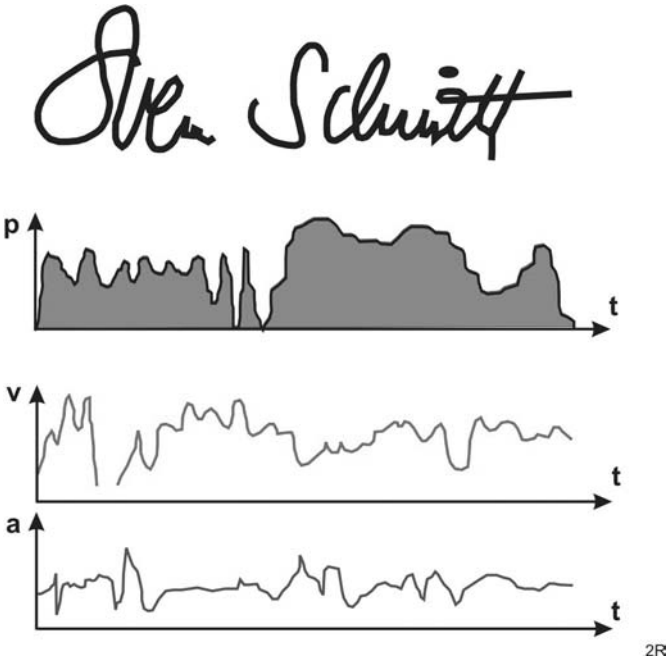
Charakteristiky on line podpisu můžeme rozdělit do dvou tříd: statistické charakteristiky a dynamické charakteristiky. Můžeme se na ně rovněž dívat jako na parametry a funkce.

Parametry jsou obvykle vyjádřeny jako vektor charakteristik $P = (p_1, p_2, \ldots, p_m)^T$, kde m je rozměr vektoru P (počet parametrů). Tyto charakteristiky jsou obvykle extrahovány v průběhu celého procesu podpisování se. Jsou to např. průměrná rychlost psaní, maximální rychlost psaní, měření vlastností zakřivení tahů, poměr dlouhých a krátkých tahů, různé délky segmentů podpisu atd.

Dynamické charakteristiky jsou vyjádřeny časovou funkcí, která charakterizuje podpis v každém časovém okamžiku jeho vzniku. Časové funkce popisují souřadnicové pozice hrotu psacího nástroje – $x(t)$, $y(t)$, rychlost $v(t)$, zrychlení $a(t)$, tlak hrotu pera na podložku $p(t)$ apod. Další metody využívají charakteristik sklonu psacího nástroje [11]. Lze rovněž využít charakteristik celkového pohybu psacího nástroje, tedy i pohyb nad papírem, kdy podpisující se osoba zvedá a spouští psací nástroj. Pohyb psacího nástroje je pak dynamicky (tj. v závislosti na čase t) zaznamenáván a vyhodnocován v třírozměrném (3D) prostoru. Hovoříme o dynamickém zdvihu. Tento přístup je poměrně netriviální na zpracování, protože je oproti zaznamenávané trajektorii podpisu na papíře absolutně neviditelný. Navíc musíme stanovit, kdy vlastně začíná samotný podpisový akt. Nemusí to být nutně okamžik, kdy hrot psacího nástroje se dotkne papíru. Trojrozměrný dynamický pohyb je pro podpisující se osobu jedinečný a napomáhá k daleko větší přesnosti metody [12].

Volba správné metody předzpracování záleží především na tom, jaké charakteristiky podpisu budeme využívat pro další zpracování. Jestliže budou použity statistické metody, proces předzpracování je poměrně jednoduchý a je primárně zaměřen na redukci nežádoucího šumu, detekci mezer (přerušení linií tahu hrotu psacího nástroje na dvourozměrné psací ploše) a normalizaci tam, kde je požadována. Zvolíme-li dynamické charakteristiky podpisu, budeme muset řešit další problémy. Proces psaní podpisu je obvykle členěn do množiny segmentů, odpovídajícím jednotlivě zvoleným charakteristikám. Tyto segmenty jsou obvykle definovány jako posloupnost paralelně běžících signálů, které vystihují jednotlivé složky podpisu – tlak hrotu psacího nástroje, souřadnice či rychlost psaní [1, 11].

Z podpisu může být extrahováno mnoho charakteristik, které určují jeho neopakovatelnost. Etapa extrakce charakteristik je důležitá i proto, abychom zvýšili výkonnost (rychlost zpracování) automatizovaného systému verifikace osoby na základě analýzy jejího podpisu. Není proto vždy vhodné pracovat se všemi charakteristikami a naopak může být výhodné snížit komplexnost úlohy a využívat jen dostatečnou, minimalizovanou množinu těch charakteristik, které v dostatečné a uspokojivé míře vyhovují požadavkům kladeným na rozlišovací schopnost systému. Statistické metody jsou běžně využívány pro výběr nezbytných charakteristik z široké množiny rozmanitých vlastností podpisu [14, 15]. V jiných systémech se naopak používají genetické algoritmy [13, 16]. Praktické zkušenosti i experimentální výsledky ukazují, že využití optimalizovaného počtu vhodně vybraných charakteristik



Obr. 11 Tlak hrotu psacího nástroje, jeho rychlost a zrychlení patří k základním atributům dynamického podpisu.

je mnohem lepší, než komplexní zpracování všech dostupných charakteristik.

2.2.2 Verifikace

V etapě verifikace před samotným verifikačním aktem musí uživatel vložit do systému své identifikační číslo ID. Systém vzápětí extrahuje množinu referenčních charakteristik, které jsou linkovány se vstupním identifikačním číslem, z referenční databáze: $R = \{R_1, R_2, \ldots, R_N\}$. Referenční charakteristiky (soubor o N charakteristikách) byly předtím vloženy do databáze v procesu pořizování vzorového podpisu. Následně se uživatel systému podepisuje prostřednictvím speciálního vstupního zařízení (tablet, elektronické pero apod.). Aplikace získává trajektorii a další vlastnosti podpisu a ukládá ji jako vzorek S. V dalším kroku je kalkulována míra ztotožnění $d(S, R_i)$ a porovnána s předdefinovaným prahem citlivosti Th[3] s cílem rozhodnout, zda akceptovat či odmítnout právě verifikovaný podpis S podle následně definovaného pravidla:

Jestliže je jedna z referencí R_i v R vyhovuje podmínce $d(S, R_i) \geq Th$, pak S je akceptováno.

V ostatních případech, každá reference R_i v R vyhovuje podmínce $d(S, R_i) < Th$, pak S je odmítnuto.

V etapě verifikace musíme řešit dva základní problémy: jak měřit míru ztotožnění mezi S a R_i a jak nastavit práh citlivosti Th.

2.2.3 Metody porovnání

Existuje několik metod pro určení míry ztotožnění mezi pořízeným a referenčním podpisem.

Metody vážené distance jsou obvykle používány ve verifikačních systémech pracujících s parametry [14, 17]. Vstupní a referenční podpis jsou vyjádřeny vektory jejich charakteristik S a R. Míra ztotožnění je pak vyjádřena pomocí vážené distance S a R:

$$d(S, R) = (S - R)^T W^{-1} (S - R) ,$$

kde W je váha diagonální matice.

Metody vážené distance jsou nejpřímější cesta k ocenění míry ztotožnění vstupního a referenčního podpisu. Váhy jsou získány z množiny tréninkových podpisů, které vznikají v průběhu registrace osoby, která aplikaci předkládá několik svých vzorových podpisů.

Statistické metody jsou popsány v [18]. Tyto metody pracují parametrickými charakteristikami s pravděpodobností $P(R|S)$ ztotožnění vstupního podpisu s podpisem referenčním. Na základě Bayesova teorému pravděpodobnost pozdějšího ztotožnění může být vyjádřena pravděpodobností předchozího ztotožnění $P(S|R)$:

$$P(R|S) = [P(S|R) \times P(R)] / P(S) .$$

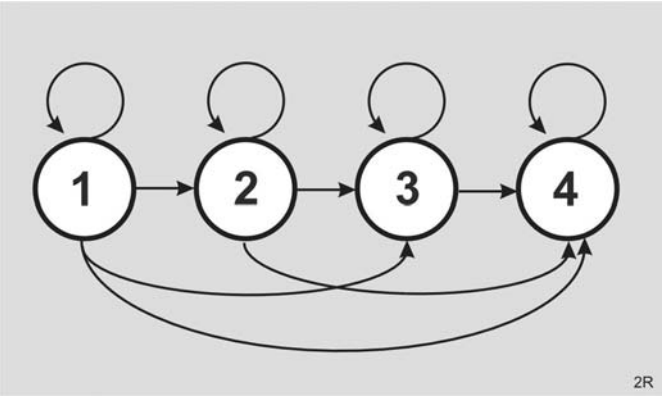
Statistické modely jsou přednastaveny za pomoci trénovacích množin podpisů uživatelů v průběhu jejich primární registrace do aplikace.

Neuronová síť využívá parametrické i funkční charakteristiky [19, 20, 21]. Neuronová síť je ve srovnání s metodami vážené distance a i s statistickými metodami mnohem přizpůsobivější. Její nelineární vlastnosti podstatně snižují chybovost nesprávného přijetí (FAR) i odmítnutí (FRR) uživatele.

Metody *dynamické časové deformace (Dynamic Time Warping – DTW)* a *skrytého Markovova modelu (Hidden Markov Model – HMM)* patří ke dvěma nejoblíbenějším metodám zpracování časově následujících signálů. Primárně byly obě metody využívány v rozpoznávání řeči a v on line systémech na rozpoznávání písma (OCR[4]) a teprve následně našly široké využití ve verifikačních systémech založených na podpisu osoby [11, 22, 23, 24, 25, 26, 27]. Metody DTW a HMM využívají především funkční charakteristiky. Velice přesně dokáží definovat podpis a jsou tolerantní k chybám oprávněné osoby (málokdo z nás se dokáže dvakrát za sebou stejně podepsat).

Ve srovnání s ostatními předchozími metodami mají navíc další výhodu. Ostatní metody totiž k vytvoření obrazu referenčního (vzorového) podpisu potřebují velké množství generovaných podpisů uživatele. Což je pro uživatele velice nepříjemné a zdržující. Metody DTW a HMM pracují s libovolně velkým počtem tréninkových podpisů. Dokonce jestliže uživatel napíše jediný podpis, ze kterého je vytvořen referenční podpis, pak i tento počet je dostatečný pro spolehlivou verifikaci. Což je obrovská výhoda pro praktické využití.

Před použitím skrytého Markovova modelu musí být podpis nejprve rozložen do jeho jednotlivých segmentů. V každém tomto segmentu se u jednotlivých jeho prvků dále pracuje s několika vybranými charakteristikami. V procesu tréninku je pro každý segment vzorového podpisu vytvořen partikulární HMM, který dále slouží jako referenční. Ve verifikačním procesu je podpis prověřované osoby opět rozložen do segmentů a k nim jsou přiřazeny partikulární HMM charakteristiky, které jsou srovnávány s charakteristikami, vytvořenými ve fázi tréninku. V praxi se používají různé modelové struktury pro HMM. Nejlepší výsledky dávají obvykle modely s „levo-pravým posuvem" – viz obr. 12.



Obr. 12 Filosofie metody MHH s levo-pravým posuvem.

2.2.4 Práh citlivosti

Problematika správné volby prahu citlivosti je velmi významná ve verifikačních systémech založených na podpisovém vzoru, neboť určuje jak celkovou výkonnost, tak i spolehlivost aplikace [1]. Jestliže

[3] *Th-Threshold* – práh citlivosti.

[4] OCR – Optical Character Recognition.

práh citlivosti *Th* je příliš nízko nastaven, poroste pravděpodobnost nesprávného přijetí (FAR), zatímco pravděpodobnost nesprávného odmítnutí bude klesat, a naopak. Volba správného nastavení práhu citlivosti je specifická pro každou aplikaci, verifikační systém. V obecných aplikacích se často setkáváme s doporučením stejného nastavení práhu citlivosti pro FAR i FRR. Ale v jiných případech, kde je kladen velký důraz na bezpečnost aplikace, je akceptace neoprávněného uživatele nepřijatelná a tomu odpovídá i specifické nastavení *Th*.

Ve většině aplikací je práh citlivosti nastaven globálně pro všechny její uživatele. Jiných, specifických aplikacích může být práh citlivosti nastaven individuálně pro každého uživatele, přičemž je garantována vysoká efektivita komplexního řešení.

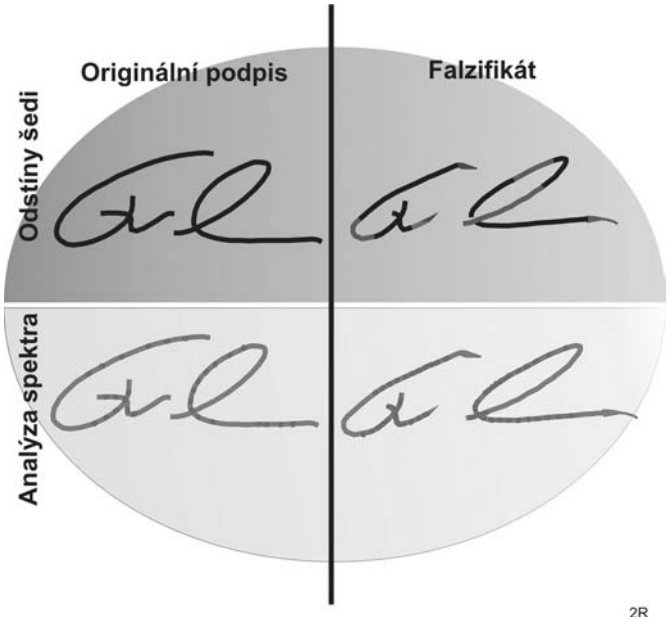
2.3 Pseudo-dynamická verifikace

Jednou z výhod moderní automatizované verifikace je schopnost rychle rozpoznávat podvrhy podpisů. Ty existují v podstatě ve dvou provedeních: napodobeniny (psané, či jinak vytvářené jinou osobou) a absolutní kopie. Kopie mohou vznikat např. skenováním či kopírováním na odpovídajícím hardwarovém zařízení. S historickým vývojem biometrických verifikačních a identifikačních technologiích se zásadně mění filozofický pohled na používané metody a přístupy, algoritmy pro výsledné porovnání. Při rozpoznávání předloženého vzorku (otisku prstu, podpisu, tváře apod.) byl před desítkami let naivně zvažován požadavek na 100% ztotožnění předloženého vzoru s jeho referenční podobou.

Moderní technologie musí umět dokázat spolehlivě rozeznat podvrh realizovaný pomocí 100% kopie originálu. Zejména při verifikaci vznikly další nároky na jejich spolehlivost, které se promítly do požadavku na tzv. „test živosti“ zkoumaného, vyhodnocovaného vzorku. Testuje se např. tělesná teplota objektu, puls krve protékající bříškem prstu, pohyb tváře, úst či očí, reakce zorničky na světelný impuls během skenování oční duhovky atd. Ve vyhodnocovacích algoritmech je dnes zakódována umělá inteligence, která zohledňuje to, že každý předložený vzorek k prověření od jedné a téže osoby může a bývá zpravidla jiný (neodchyluje se ale od určitého statistického průměru). Téměř nikdy se nepodepíšeme stejně, palec či jiný prst, který zanechává otisk, taktéž nepřiložíme na podložku pod stejným úhlem, tlakem. Otisk může být deformován „krutem“ prstu při kontaktu s povrchem. Vzhled naší tváře se mění s přibývajícím stářím, stejně tak hlas může být momentálně ovlivněn nejenom okolním šumem, ale i naší dočasnou indispozicí, nachlazením apod.

Jestliže tyto vlastnosti v minulém století bránily ztotožnění (verifikačnímu nebo identifikačnímu verdiktu), nyní mohou velice intenzivně napomáhat k odhalení podvrhu. Požadavek na absolutní shodu předkládaného vzoru se vzorem referenčním ve vztahu 1:1 není proto dnes správným přístupem k navrhování vyhodnocovacích algoritmů. Naopak – 100% shoda ve všech kritériích bývá mnohdy podezřelá a nasvědčuje podvrhu.

Dynamický podpis již sám v sobě obsahuje prvek „živosti“ objektu (pisatele), takže není potřeba vyvíjet další mechanismy testující, zda objekt je živý či nikoliv. Pohyb hrotu psacího nástroje v trojrozměrném prostory (kde kromě souřadnic *x, y, z*) se snímá tlak psacího nástroje na podložku *p*, rychlost písma *v*, zrychlení *a* či časové intervaly mezi jednotlivými částmi podpisu (např. jméno, příjmení). Verifikace osoby na základě jejího podpis je



Obr. 13 Filosofie rozpoznávání padělku pomocí pseudo-dynamických přístupů.

jedna z nejpřirozenějších biometrických metod, protože jsme dennodenně zvyklí cokoliv stvrzovat naším podpisem. Metoda nikoho nijak neobtěžuje jak po stránce technické, tak i společenské či kulturní.

V praxi se kromě čistě statistických nebo dynamických metod pro vyhodnocování otisku můžeme setkat i s přístupy *pseudo-dynamickými*.

S využitím statistických metod a vlastností elektronického obrazu prvku podpisu můžeme odvozeně usuzovat i o určitých dynamických rysech podpisu. Jsou to především derivované charakteristiky tlaku hrotu psacího nástroje a jeho rychlost. Technologie vycházející z různých odstínů šedi trajektorie podpisu v některých praktických přístupech (např. produkt *Automatic Forgery Detection Sign Check* německé firmy *Softpro*) dokáží rozlišovat až 240 nejrůznějších specifických charakteristik podpisu.

Na základě vyhodnocením vrstev inkoustu (či jiné psací hmoty) lze odvodit nezbytné relativní dynamické parametry. Technologická vizualizace drobných nuancí zkoumaných parametrů dokáže odhalit napodobeniny či kopie podpisu, které nejsme schopni postihnout pouhým lidským okem.

2.4 Snímací periférie

S rozvojem technologických možností se časem mění pohled na aplikační SW i na hardware. Typická je miniaturizace a orientace na uživatelský komfort.

První zařízení byla vyvíjena na základě grafických tabletů, používaných ke kreslení ve standardních grafických editorech. Zařízení byla upravována tak, aby se co nejlépe přibližovala klasickému psacímu peru. Tak jak se vyvíjel pohled na využití statických a dynamických metod, akcent byl stále více kladen na měření dynamických parametrů – tlaku, rychlosti, zrychlení. U klasických tabletů bylo pero spojeno s počítačem pevným vodičem, což znepříjemňovalo uživatelský komfort a ovlivňovalo psychiku pisatele.

Obr. 14 Ukázka staršího grafického tabletu pro podpis.

Byla proto vyvíjena speciální pera, která data přenášela bezdrátově do vstupní jednotky a dále pak do počítače. Tato pera, ač jsou schopna snímat mnoho dynamických parametrů, jsou pro uživatele téměř nerozlišitelná od běžných psacích nástrojů používaných v běžném občanském životě.

Jiným možným řešením je snímání podpisu přímo na obrazovce PDA[5)] zařízeních, které jsou vybaveny speciálním psacím hrotem.

V praxi se můžeme setkat i se speciálními psacími nástroji, které snímají otisk ukazováčku. Tato zařízení verifikují podpisující se osobu na základě otisku prstu a jsou koncipována pro garanci spojení pisatele s elektronickým dokumentem. Biometrické pero Pen One není v tomto případě nikterak využíváno pro verifikaci osoby na základě jejího podpisu.

2.4.1 Oblasti praktického využití

Pro široké nasazení každé nové technologie je rovněž rozhodující její zakotvení v právní oblasti. Legislativa vztahující se k digitalizovanému lidskému podpisu se v Evropské unii a ve Spojených státech amerických liší.

V EU autor elektronického podpisu podle příslušné legislativy vyjadřuje svůj souhlas s obsahem digitálního dokumentu. Biometrické charakteristiky – v našem případě podpis – jsou nyní zatím chápány jako volitelný, doplňkový prostředek k autentizaci a ve srovnání s metodami založenými na personálních

Obr. 15 Řez speciálním perem SmartPen, umožňujícího snímání dynamických charakteristik. V koncové části je zabudována elektronické část s mikrovysílačem naměřených hodnot, charakterizujících podpis.

Obr. 16 Pero Pen-One je prvním psacím perem s integrovaným snímačem otisku prstu- Otisk je snímán 0,25" palcovým čtvercovým senzorem firmy AuthenTec.

identifikačních číslech (PIN) jsou vnímány proto jako druhořadé.

V USA, na základě zákonného aktu SB 761 (*Electronic Signature Global and National Commerce Act*[6)]) má elektronický podpis (v jakékoliv své podobě, tedy i ručně psaný a elektronicky snímaný) stejný právní status, jako ruční podpis psacím nástrojem na papíře. Zákon je platný v USA od října 2000.

Přijatelnost metody založené na podpisu osoby

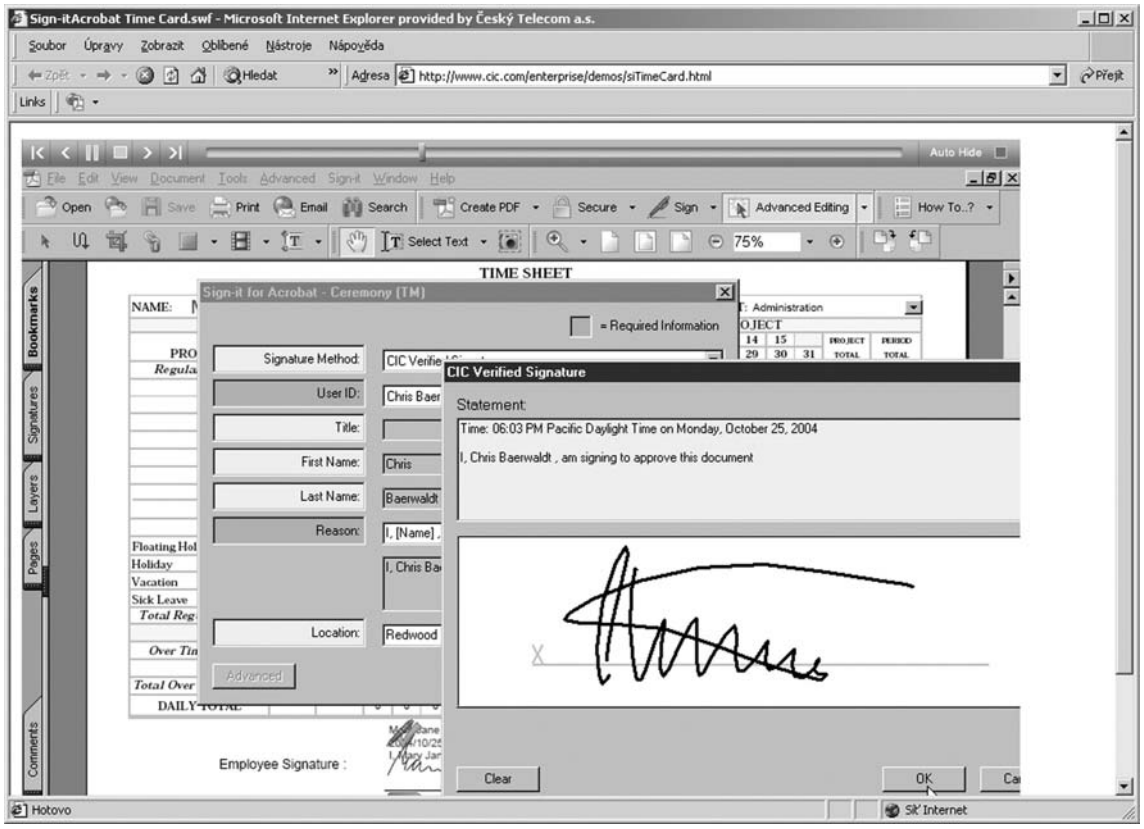
Existuje řada důvodů, proč verifikace osoby založené na jejím podpisu patří k nejoblíbenějším prostředkům autentizace. Podpis obsahuje aktivní biometrické charakteristiky, které nevznikají náhodně. Mají dynamický charakter vycházející z fyziologických a biomechanických schopností a z procesu individuálního se učení, čímž se principiálně liší od pasivních biometrických metod, založených na geometrických tvarech či jejich rozměrech. Dynamický podpis může snadno realizovat i test „živosti“ verifikované osoby.

Ekonomičnost

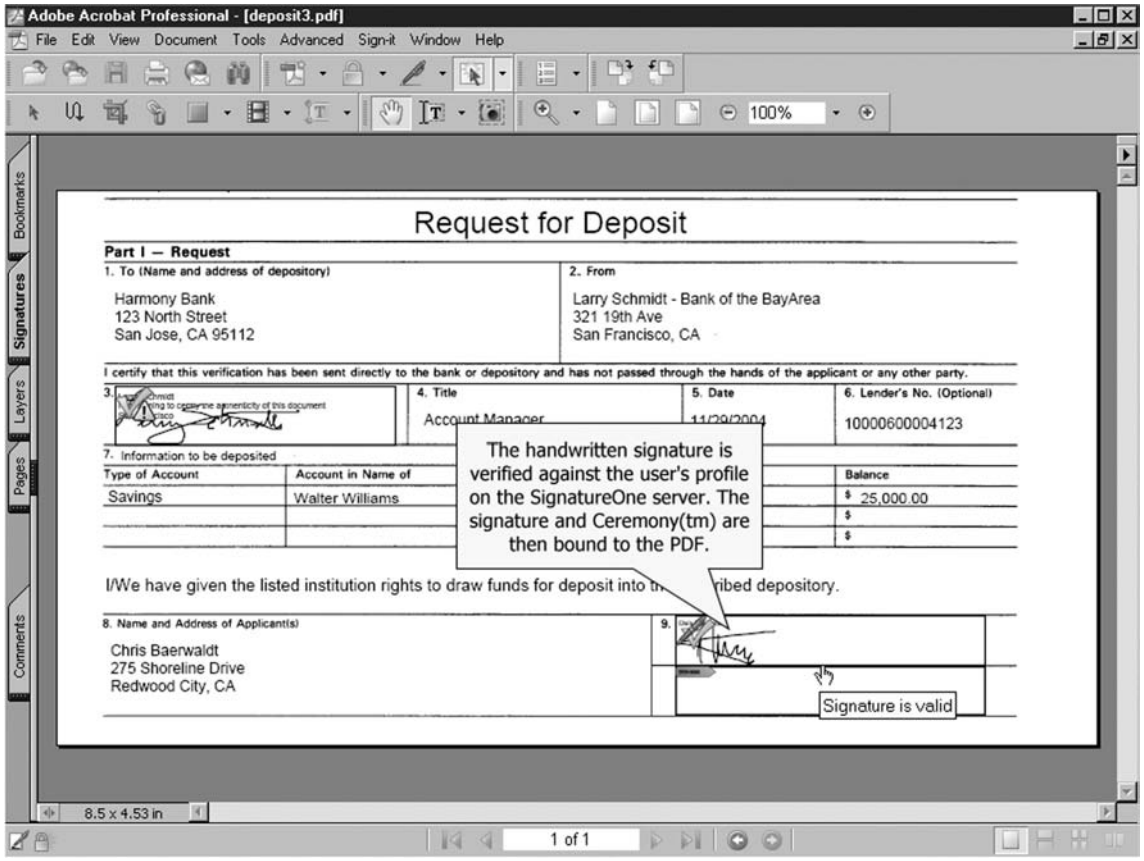
Metoda elektronicky snímaného a vyhodnocovaného podpisu šetří papír a další náklady např. na skenování podpisu. Skenování podpisu se používalo ještě zcela nedávno (mnohdy dosud) pro potřeby uchování vzorového podpisu v jeho grafické, statické podobě např. v bankovních aplikacích. Zkracuje čas zavedení/

[5)] PDA – Personal Digital Assistent.

[6)] Známý v USA též pod názvem *e-SIGN bill*.



Obr. 17 Akt samotného stvrzení dokumentu podpisem.



Obr. 18 Verifikace uživatelova podpisu a spojení jeho identity s podepsaným dokumentem.

updatu referenčního podpisu v aplikaci. Umožňuje on-line verifikaci osoby prostřednictvím internetové sítě.

Integrační metody jsou orientovány zejména na následující technologické platformy:

- Internetový prohlížeč.
- Adobe Acrobate PDF formát .
- Microsoft Word dokumenty.
- Zákaznické aplikace, orientované i na formuláře.
- Operační systémy Win2000/XP, Unix, Palm OS a další.

3. LITERATURA

[1] R. Plamondon and G. Loretce: „*Automatic Signature Verification and Writer Identification – The State of the Art*“, Pattern Recognication, vol. 1, No.2, pp. 107–131, 1989.

[2] D.D. Zhang: "*Automated biometrics Technologies and Systems*", Kluwer Academic Publishiers, 330 pp, ISBN 0-7923-7856-3.

[3] J. Duvernoy: "*Handwritting synthesis and Classification by Means of Space Variant Transform and Karhunen-Loeve Analysis*", J. Opt. Soc. Am., pp. 1331–1336, 1975.

[4] N. Papamarkos and H. Baltzakis: "*Off line Signature Verification Using Multiple Neural Network Classification Structures*", Proceedings of 13th International on Digital Signal Processing, 1997.

[5] K. Han and I.K.Sethi: "*Handwritten Signature Retrieval and Identification*", Pattern Recognition Letters, vol. 17, pp. 83–90, 0167–8655/96, 1996.

[6] M. Dehghan, K. Faez and M. Fathi: "*Signature Verification Using Shape Descriptors and Multiple Neural Networks*", TENCON ´ 97., IEEE Region 10 Annual Conference, Sérech and Image Technologies for Computing and Telecommunication, Proceedings of IEEE, vol. 1, pp. 415–418, 1997.

[7] J. Lin and J. G. Li: "*Off line Chinese Signature Verification*", Proceedings, pp. 364–381, Wold Scientific Publishing Co. Pte. Ltd., Singapore, 1997.

[8] http://www.signplus.com/doc

[9] G. Dimauro, S. Impedovo, G. Pirlo and A. Salzo: „*A multi-expert Signature Verification for Bankcheck Processing*“, Automatic Bankcheck Processing, pp. 364–381, World Scientific Publishing Co. Pte.Ltd., Singapore, 1997.

[10] R. Sabourin and G. Genest: "*An Extended-Shadow-Code based Approach for Off-Line Signature Verification: Part II – Evaluation of Several Multi-Classifier Combination Strategies*", Proc. ICDAR, Ulm, IEEE, 1995.

[11] K. Huang and H.Yan: „*On-line Signature Verification Based on Dynamic Segmentation and Global and Local Matching*“, Optical Engineering, vol. 34, No 12, pp. 3480–3487, 1995.

[12] J. G. A. Dolfing, E. H. L. Aarts,V. Oosterhout: "*On-line Signature Verification with Hidden Markov Models*", Proceedings of 14th International Conference on Pattern Recognition", 1998.

[13] X. H. Yang, T. Furuhashi, K. Obata and Y. Uchikawa: "*Constructing a High Performance Signature Verification System Using a GA Method*", Proceedings of the Second New Zealand Two-Stream International Conference on Artificial Neural Networks and Expert Systems (ANNES 1995), 0-8186-7174-2/95 IEEE, 1995.

[14] F. Bauer and B. Wirtz: "*Parameter Reduction and Personalized Parameter Selection for Automatic Signature Verification*", Proc. ICDAR, Ulm, IEEE, 1995.

[15] L. L. Lee, T. Berger, E. Aviczer: "*Reliable On-line Human Signature Verification Systems*", IEEE Transactions on Patern Analysis and Machine Intelligence, vol. 18, No 6, 0162-8828/96, IEEE 1996, June 1996.

[16] G. S. K Fung, J. N. K. Liu, R. W. H. Lau: "*Feature Selection in Automatic Signature Verification Based on Genetic Algorithms*", Proceedings of the International Conference on Neural Information Processing, Progress in Neural Information Processing, Amari, et al. (Eds), pp.811–815, Springer-Verlag, 1996.

[17] R. Martens, L. Claesen: "*On-line Signature Verification: Discrimination Emphasised*", Proc. ICDAR, Ulm, IEEE, 1997.

[18] B. Herbst, D. Richards: "*On an Automated Signature Verification System*", Proceedings of IEEE International Symposium on Industrial Electronics, 1998.

[19] L. L. Lee: "*Neural Approaches for Human Signature Verification*", Proc. ICDAR, Ulm, IEEE 1995. The 3rd International Conference on Signal Processing, 1996.

[20] G. B. Hesketh: "*COUNTERMATCH: A Neural Networks for Industrial Applications*" (Digest No 1997/04).

[21] N. Mohankrishnan, W. S. Lee and M. J. Paulik: "*Multi-Layer Neural Network Classification of On-Line Signatures*", IEEE 39th Midwest Symposium on Circuits and Systems, 1996.

[22] R. Martens and L. Claesen: "*On-line Signature Verification by Dynamic Time Warping*", Proceedings of 13th International Conference on Pattern Recognition, 1015–4651/96, 1996.

[23] R. Martens and L.Claesen: "*Dynamic Programming Optimization for On-line Signature Verification"*, Proceeding of 4th ICDAR ´ 97. 0-8186-7898-7/97, 1997.

[24] B. Wirtz: *"Stroke-Based Time Warping for Signature Verification",* Proc. ICDAR, Ulm, IEEE, 1995.

[25] W.S.Lee, N. Mohankrishnan and M.J.Paulik: *"Improved Segmentation Through Dynamic Time Warping for Signature Verification Using Neural Network Classifier"*. Proceedings of 1998 International Conference on Image Processing, 1998.

[26] B. Wirtz: *"Average Prototypes for Stroke-Based Signature Verification",* Proceeding of 4th ICDAR ´ 97. 0-8186-7898-7/97, 1997.

[27] C.C. Hsu, L.F. Chen, P.C. Change and B.S.Jeng: *"On-line Chinese Signature Verification Based on Multiexpert Strategy"*, Proceedings of 32nd Annual 1998 International Carnahan Conference on Security Technology", 1998.

[28] www.pen-one.com